PCT/GB 2003 / 002074

The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed R. Mahoney

Dated 30 MAY 2003

Patents Form 1/77

Pat[illegible]t 1977
(Rule 16)

THE PATENT OFFICE
A
13 JUN 2002
LONDON

The Patent Office

14JUN02 E725671-1 D02855
P01/7700 0.00-0213609.1

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference 24/P32627GB

2. Patent application number *(The Patent Office will fill in this part)* 0213609.1

13 JUN 2002

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

VODAFONE GROUP PLC
THE COURTYARD
2-4 LONDON ROAD, NEWBURY
BERKSHIRE
RG14 1JX

Patents ADP number *(if you know it)* 8154718001

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention

NETWORKS

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

MATHISEN, MACARA & CO
The Coach House
6-8 Swakeleys Road
Ickenham, Uxbridge
UB10 8BZ

Patents ADP number *(if you know it)* 1073001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number	Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	17 ✓
Claim(s)	4 ✓ CF
Abstract	1 ✓
Drawing(s)	4 + 4

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1 ✓
Request for preliminary examination and search *(Patents Form 9/77)*	1 ✓
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature: Mathisen, Macara & CO

Date: 13 JUNE 2002

12. Name and daytime telephone number of person to contact in the United Kingdom: MARK C FOSTER 01895 678331

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

DUPLICATE

UK PATENT APPLICATION

APPLICANTS: VODAFONE GROUP PLC

SHORT TITLE: "PSD"

REFERENCE: P32627GB

FORMAL TITLE: NETWORKS

APPLICATION No:

FILED:

PRIORITY CLAIMED: NIL

MATHISEN, MACARA & CO
The Coach House
6-8 Swakeleys Road
Ickenham, Uxbridge
England, UB10 8BZ

Agents for the Applicants

F:020613

NETWORKS

The present invention relates to a network including a plurality of devices, each device being capable of wireless communication with the other devices of the network, and to a method allowing selected devices within a network to be associated within a domain.

According to the present invention, there is provided a network including a plurality of devices, each device being capable of wireless communication with the other devices of the network, and wherein one of the devices includes administration means for allowing selected devices to be associated within a domain by providing each device with identification data, the identification data of each device being interpretable by each other device within the domain, particular modes of communication only being allowed between devices within the domain having such identification data.

According to another aspect of the present invention, there is provided a method allowing selected devices within a network to be associated within a domain, each device being capable of wireless communication with the other devices of the domain, the method including adapting one device within the domain to provide each other device with identification data, the identification data of each device being interpretable by each other device within the domain, particular

modes of communication only being allowed between devices within the domain having such identification data.

For a better understanding of the present invention, embodiments will now be described by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows a personal area network (PAN) including a plurality of devices belonging to one user;

Figure 2 shows a personal area network (PAN) having two PAN Security Domains (PSDs) formed therein in accordance with the invention;

Figure 3 shows the formation of a further PSD in the PAN of Figure 2; and

Figure 4 shows the exchange of data between devices within a PSD.

Figure 1 shows a personal area network (PAN) 1 including a plurality of devices belonging to one user. Within the PAN 1 it is desired that all the individual devices can communicate and share resources with other devices of the same user in seamless fashion. From a security standpoint, this requires individual devices to identify other devices owned by the same user when offering or requesting services. Further, in order to protect data confidentiality, individual

devices should be able to communicate securely with each other. Depending on the number of devices within the PAN 1 and the services they offer, this can become very complicated. This problem is further complicated because the number of devices will be changing with time as devices join and leave the PAN 1.

A PAN is different from a conventional network in that communication between devices is not through a server.

If such a multitude of devices in a PAN are expected to have coherent behaviour, all devices should be able to fit into a distributed terminal architecture capable of taking into consideration the ownership and privileges required for individual devices to operate.

In Figure 1 the devices in the personal area network 1 comprise a GPRS mobile telephone 3, laptop computer 5 and personal digital assistant (PDA) device 7. As indicated by the arrows, each of the devices 3, 5, 7 is capable of communicating with the other devices within the PAN 1. In this example each of the devices 3, 5, 7 is a Bluetooth device, allowing the devices 3, 5, 7 to be inter-operable. Data communication between the devices 3, 5, and 7 may be by infrared communication, radio communication or by any other wirelcss means.

For example, the PDA 7 will connect to the mobile telephone 3 to access the Internet and to the laptop computer 5 to synchronise the user's calendar or to exchange files for other reasons.

Conventionally, each pair of devices 3, 5 and 7 must be separately configured to communicate with each other. This will require three separate configuration processes, for example between the laptop 5 and the PDA 7, the laptop 5 and the mobile telephone 3 and the mobile telephone 3 and the PDA 7. After an initial configuration processes the devices 3, 5, 7 may communicate with one another, although typically this will require the user to manually select a communication mode on each of two devices to communicate with one another. The devices may be configured to require the user to enter a personal identification number (PIN) before data exchange between a pair of devices can begin in order to, for example, prevent an unwanted device being substituted for one of the devices 3, 5 and 7 and obtaining or over-writing data from a device within the PAN 1.

In such a PAN 1, if it is desired to add a further device, such as MP3 player 9, it will be necessary to configure separately each of the devices 3, 5, 7 within the PAN 1 to communicate with the MP3 player 9. It will be appreciated that, as the number of devices within the PAN 1 increases, the addition of a new device to the PAN 1 requires an increasing number of configuration steps. For a conventional PAN having n components, $n*(n-1)/2$ component associations must be performed to form the PAN.

According to an aspect of the invention a group of devices within a PAN form a PAN Security Domain (PSD). A PSD is a group of components inside a PAN where each component can be authenticated, trusted and securely communicated with by means of some common security association. This reduces the number of component association procedures required.

In a PSD one device has the role of a PSD administrator. This device includes security data (for example a shared key or a public-private key pair) that can be selectively passed to other devices that are to join the PSD. Communication can only successfully occur between devices that have this security data. Once a device has the security data, it can communicate with other devices in the PSD without referring to the PSD administrator. When a device is added to the PSD the PSD administrator advises each device of the addition of a new device to the PSD. If there are n devices in the PSD this requires n-1 inter-device communications. It is not necessary for the new device to separately pair or associate itself with each other device in the PSD.

The security association could be in the form of a shared secret key or a shared group key based on public key techniques, with a mutual "trust" being established between the devices by a personal certification authority (CA) within the PSD. Certificates issued to all PSD members indicate the device as a member of that PSD. The group key is not used for secure bilateral communications in

the PSD, which takes place using bilaterally established keys (discussed further below). The group key is used only for proof of PSD membership, secure PSD-wide broadcasts and PSD-wide secure communications.

The initial decision as to whether a device can be part of a PSD or not will be on user judgement followed up by positive authentication of the device based on a public key infrastructure (PKI) trusted root certificate. Alternatively, another known authentication method could be used.

One device within the PSD is nominated as the PSD administrator. The PSD administrator is a role that could be assumed by any of the devices in the PSD provided it contains the necessary hardware to support the role, for example a secure key store and/or a display. The administrator role may be moved from one device to another. If the administrator role is moved to a new device, the new device will have passed thereto, or have pre-stored thereon, the necessary security data to allow the admission of new devices to the PSD.

The PSD administrator also is responsible for configuring and managing the policies (described below) governing the devices in the PSD. Additionally it is responsible for enrolling new members in the PSD. The PSD administrator could also contain the personal CA that is responsible for issuing certificates to the PSD members. Advantageously, the PSD administrator will be the device with

the greatest processing power and the best user interface. In a PSD based on the PAN 1 of Figure 1, the administrator is laptop 5.

When a single user owns all devices in a PSD and treats them equally, such a configuration of devices will not contain any restrictions based on the identity of a device. All shared resources will be made available to all the PSD member devices. In other words, there is group "trust" between the devices. If a device is a member of the PSD, the other devices will assume that the devices can be trusted and communicated with. There is no need for each device to set up an individual trust relationship with each other device, in contrast to a conventional PAN as described above. Provided that the device is admitted to the group by the PSD administrator, the other devices will assume that the newly-admitted device can be trusted.

Figure 2 illustrates a PAN 11 containing six devices, designated A to F. The devices shown in Figure 2 are all PDAs but it should be understood that they could be other types of device, or a combination of different devices, as in Figure 1. Devices A, B and C are owned by the same user (user 1) while D and E are owned by another user (user 2). A third user (user 3) owns device F. All these devices are capable of communicating with other using their local interfaces.

A first PSD 13 includes devices A, B and C. These devices will be able to share resources and communicate with each other securely. A second PSD 15 includes

devices D and E. Again, these devices will be able to share resources and communicate with each other securely.

If membership of one PSD is limited to devices, such as devices A, B and C, from a single user, two users will not be able share any resources. Sharing of resources could be achieved if the existing PSDs are configured so that device sharing between the PSDs is possible.

A more effective and preferred way for the two users to share resources is to establish a new PSD. Depending on the situation, this PSD could be a temporary or a permanent PSD including the devices with the resources required to be shared.

Figure 3 shows a new PSD 17 formed between devices B, C and E. This will require a security association between two devices belonging to users 1 and 2. This association does not have to be between the very same devices that are going to be part of the new PSD. The original PSD could transmit the necessary data to introduce the new device to the PSD to all its member devices. Alternatively, the users 1 and 2 could pair two devices (one from each user) and then add further devices as required using one of the original devices as the PSD administrator.

When forming a PSD with devices from different users, it is not always straightforward to assign a PSD administrator. It might have to be mutually agreed by all parties in the PSD. Alternatively, the device that initially created the PSD could assume this role. Nevertheless, if required it could be handed over to another device in the PSD.

Each user can then configure their device policies to share the required resources with the members of the newly formed PSD.

User 1 will configure the policy on B and C while user 2 will do the same for E. Individual devices could contain a number of built in or preset configurations that could be activated by the user for different PSDs.

If required a PSD could also be used to establish different groups within a set of devices owned by the same user.

In addition to the temporary PSD between user 1 and user 2, either of them could establish another PSD to share resources with user 3. In order to keep the PSD concept simple, user 2 cannot use one of his devices, say E to establish a PSD between user 1 and 3, i.e. E cannot bridge the trust between the two different PSDs. Nonetheless, this could be achieved if E used as a PSD administrator to form a PSD involving devices from user 1 and user 3.

The formation of a PSD between devices B, C and E, with identities IDB, IDC and IDE respectively, will now be described in more detail, with reference to Figure 4. In order for these devices to form a PSD, two security associations between the three devices are needed. For example, these could be {B, C} and {C, E}. Based on these associations, it is possible for B and C, and C and E to communicate securely. Device C performs the role of PSD administrator. C then generates a group PSD membership key KPSD. C then communicates the identities of all PSD members to each other, i.e. forwards IDB and IDE to E and B respectively. Together with KPSD, B and E are now in a position to generate a further key KBE to allow secure communications between them. Figure 4 of the drawings shows the exchange of data between devices.

Alternatively, device C can have the role of a personal CA and issue B and E with certificates to carry out the above key exchanges using a local PKI. The possession of this certificate is equivalent to having access to KPSD, i.e. its proof of membership in the PSD.

However, forming a PSD itself does not impose any behaviour patterns or rules on the individual devices themselves. These must be achieved through a suitable "policy". This policy will set guidelines on behaviour and dictate how resources should be used and how the device should behave under different circumstances.

PSD policy can be used to enforce restrictions on any of the following:

a. Access to resources and their usage patters.

b. Requirements for joining the PSD as a member.

c. Requirements to assume the role of the PSD administrator.

d. User interaction.

e. Usage of chargeable services.

f. Usage of user private information.

Devices from more than one user may be PSD members.

The PSD policy file is in a standardised format to achieve interoperability between devices and it contains information about the resources available to different devices depending on the PSD to which they belong. All the resources listed in the file do not have to be available to the PSD all the time. These entries can be for future use when the resource is available to the PSD.

Each device has its own version of the policy file that states which resources are available from that particular device to the rest of the PSD members. Hence the policy file for two devices with different resource commitments to the PSD will differ. Devices may update or modify this as and when resources are either added to the PSD or removed from the PSD. Alternatively, the device might rely on the PSD administrator to do this on the device's behalf.

Depending on the access control mechanism it might be required to the store the policy file locally on a device. Nevertheless it is possible for a device to enquire and obtain policy information from a trusted device. It is not required for this trusted device to be a member of the same PSD.

The significance of each entry in a device policy is explained below.

Resource Type & ID	Target ID	Authorisation ID	Permission Type	Validity
GPRS	C		Component	1 day
....	...	...	...	...

An Example PSD Policy File

Resource Type & ID

This contains information about the ID of the resource and its type. The ID is required to uniquely identify the resource within a component. The type of the resource is important when enforcing "Permissions Types" (discussed below) applicable to a resource.

Different resources on a component can be divided into four broad functional areas depending on their impact on the hosting component and its user.

1. Local Services - Printers, projectors, etc.

2. Network Interfaces - GSM, GPRS, BT, IrDA, WLAN, etc., or similar resources related network connectivity

3. Personal Information Management - Calendar, Phonebook, Location information etc., which are of personal value and will have privacy issues associated with them.

4. Executables - refers to code downloaded from another component on to the target device.

The above is merely an example of resources.

Target ID

Uniquely identifies the component where the resource is located. It is useful to identify resources within the PSD when the resource is available from more than one component in the PSD.

Authorisation ID

PSD members have access to all PSD resources that have been made available by the policy file. If the PSD relies on a PSD administrator, then the Authorisation ID should be the ID of the component assuming the role of the PSD administrator. If the component is to have the autonomy to authorise other components access to its resources, then the Authorisation ID is the same as the Target ID. When there are devices from more than one user, it is likely that the

devices will retain the ability to authorise themselves without having to rely on a PSD administrator.

Permission Types

The permission types that are made available to different components depend on the resource type and other considerations. In order to cater for different usage scenarios and patterns there are different permissions types depending on the type of the resource.

a. Component - Will use the targeted component's default access control rules applicable for a component of given trust level. The component's local security policy is consulted when making the access control the decision.

b. User - Will prompt the user to grant permission from a range of permissions types available for a device of that trust level.

c. Allowed - The indicated resource is given access to the resource until further notice

Furthermore, if the selected permissions type is "user", the PSD policy file should contain a user permission type.

Validity

Contains information on validity periods for which a request can be granted to components of various trust levels.

Each device within a PSD may be equally trusted, i.e. all devices within a PSD will have access to the same information. Alternatively, devices within a PSD may have different "privileges", that is one device may be able to access information that another device within the PSD is prevented from accessing. For example, a PSD may include two personal computers, PC A and PC B. These personal computers could be configured so that only PC A has access to the PSD user's e-mails (which could be stored on PC A or elsewhere). Such restrictions (or privileges) to the access of information within the PSD could be held on the policy file for that PSD). It is preferred that the restrictions or privileges can be changed within a PSD, as required. This will typically be performed under control of the PSD administrator.

The advantages of a PSD include:

* It is not necessary for a new PSD member to share security associations with all existing PSD members to establish trusted communications with them. For example, if device D joins an existing PSD of A, B and C, which is defined by group key, KABC. Once D has been authenticated by A (the PSD administrator), and a bilateral communication key KAD established, A can send KABC to D under the protection of key KAD. D

can then prove PSD membership with this and establish further bilateral secure communication keys with B and C.

* Reduction in the user interaction required as the number of imprinting events is reduced. For a PSD of n components, only n-1 imprinting sessions are necessary, compared to $n(n-1)/2$ in a conventional PAN without the PSD concept
* Use of the device with the best user interface for the PSD administrator for enrolling new members allows the most user friendly imprinting protocols to always be used
* Use of a PSD administrator with revocation checking facilities allows revocation checks to be performed when new devices with certificates are enrolled
* Consistent resource information across all devices
* Resources can be shared with other users without having to compromise interactions between one's own devices
* Designation of group roles:
    - o Designation of a single device to perform the role of a gateway between all PSD devices and external devices.
    - o Designation of devices to perform specialised tasks, for example calendar synchronisation, revocation checking
* Use of the shared security associations to perform secure broadcast
* A device can be nominated by the user to perform administrative tasks on his behalf, i.e. the PSD administrator

* Establishes another layer of security on top of link layer security
* Different PSDs can be created for different trust groups within a PAN to solve particular access control problems.

The PSD concept described above is applicable to networks other than PANs. The devices in the network (and domain) may be separated by large distances.

Devices could be manufactured or pre-configured to enrol in certain PSDs automatically. For example, a mobile telephone could be configured so that when it comes within communication range of a particular PSD it automatically enrols in that PSD. Where such automatic enrolment is provided, generally the exchange of data between devices in the PSD will be restricted to prevent private information being disclosed to other devices in the PSD.

For example, a PSD could be arranged by a train operating company that automatically enrolled appropriately programmed mobile telephones at a station so that train running information can be transmitted to the telephone for use by the user.

CLAIMS

1. A network including a plurality of devices, each device being capable of wireless communication with the other devices of the network, and wherein one of the devices includes administration means for allowing selected devices to be associated within a domain by providing each device with identification data, the identification data of each device being interpretable by each other device within the domain, particular modes of communication only being allowed between devices within the domain having such identification data.

2. The network of claim 1, wherein the identification data received from the administration means includes a key.

3. The network of claim 2, wherein the key is a shared key.

4. The network of claim 2, wherein the key is a public key of a public-private key pair, the private key being stored on the administration means.

5. The network of any one of claims 1 to 4, wherein each device has a security certificate associated therewith indicating its membership of the domain.

6. The network of any one of claims 2 to 5, including further keys for allowing encrypted communication between the devices within the domain.

7. The network of any one of claims 1 to 6, wherein the administration means transmits to each device within the domain data indicative of the characteristics of the other devices within the domain.

8. The network of any one of claims 1 to 7, wherein the administration means is transferable form one device to another.

9. The network of any one of claims 1 to 7, wherein a plurality of devices within the domain include administration means, and means is provided to selectively enable only one of said administration means at a time.

10. The network of any one of claims 1 to 9, including a plurality of said domains.

11. The network of claim 10, wherein a device is associated with each of said plurality of domains.

12. A network substantially as hereinbefore described and/or substantially as illustrated in any one of or any combination of the accompanying drawings.

13. A method allowing selected devices within a network to be associated within a domain, each device being capable of wireless communication with the other devices of the domain, the method including adapting one device within the domain to provide each other device with identification data, the identification data of each device being interpretable by each other device within the domain, particular modes of communication only being allowed between devices within the domain having such identification data.

14. The method of claim 13, wherein the identification data includes a key.

15. The method of claim 14, wherein the key is a shared key.

16. The method of claim 14, wherein the key is a public key of a public-private key pair, the private key being stored on the adapted device.

17. The method of any one of claims 13 to 16, wherein each device has a security certificate associated therewith indicating its membership of the domain.

18. The method of any one of claims 14 to 17, including providing further keys for allowing encrypted communication between the devices within the domain.

19. The method of any one of claims 13 to 18, wherein the adapted device transmits to each device within the domain data indicative of the characteristics of the other devices within the domain.

20. The method of any one of claims 13 to 19, including changing the device within the domain which provides each other device with identification data.

21. The method of any one of claims 13 to 20, including allowing the formation of a plurality of said domains.

22. The method of claim 21, wherein a device is associated with each of said plurality of domains.

23. A method substantially as hereinbefore described and/or substantially as illustrated in any one of or any combination of the accompanying drawings.

ABSTRACT

NETWORKS

A network 11 including a plurality of devices A...F, each device being capable of wireless communication with the other devices of the network. One of the devices C includes administration means for allowing selected devices A,B,C to be associated within a domain 13 by providing each device A,B,C with identification data, the identification data of each device being interpretable by each other device within the domain, communication only being allowed between devices within the domain having such identification data.

[Figure 3]